Detection And Prevention Of Types Of Attacks Using Machine Learning Techniques In Cognitive Radio Networks

SUDHA Y

Assistant Professor, Department of Computer Science and Engineering, Presidency University, Bengaluru

Abstract: **A number of studies have been done on several types of data link and network layer attacks and defenses for CSS in CRNs, but there are still a number of challenges unsolved and open issues waiting for solutions. Specifically, from the perspective of attackers, when launching the attack, users have to take into account of the factors of attack gain, attack cost and attack risk, together. From the perspective of defenders, there are also three aspects deserving consideration: defense reliability, defense efficiency and defense universality. The attacks and defenses are mutually coupled from each other. Attackers need to adjust their strategies to keep their negative effects on final decisions and avoid defenders' detection, while defenders have to learn and analyze attack behaviors and designs effective defense rules. Indeed, attack and defense ought to be considered together. the proposed methodology overcomes the problems of several data link and network layer attacks and it effects in CSS(Co-operative Spectrum Sensing) of CNRs using Machine Learning based Defense, Cross layers optimization techniques and Defence based Prevention mechanisms.**

Keywords: **Cognitive Radio Networks (CRN); SSDF; DOS; WRSNN's; Cognitive Radio Wireless Sensor Node Networks (CRWSNN's);**

I. INTRODUCTION

The wireless communications are generating the spectrum shortage problems with the Reference to the latest developments. The more challenges in the use of licensed wireless networks or unlicensed wireless networks with opportunistic use of the spectrum with limited rules or without limited rules. The different frequency bands are used by different wireless networks. So it's very important to use attenuation bands when there is no activity occurs on them. A new technology which leads like Cognitive radio is to solve these problems through dynamically utilization of rules and spectrum. Several spectrum sharing schemes have been proposed in cognitive radio. The major and challenging issues are security in cognitive radio network. The attackers in cognitive radio technology as compared to the wireless networks in a general form chances are pre- arranged. Mobile station equipment may switch to any available frequency band in the cognitive radio, and make list of free channel and take handoff decision. So whenever handoff is made there will be a chance that malicious attacker may hack ongoing traffic. He may even break off established traffic by imitating any kind of active or passive attack like spoofing denial of ser- vice, interception etc. Cognitive Radio (CR) is an enabling technology to effectively address the spectrum scarcity and it will significantly enhance the spectrum utilization of future wireless communications systems. In a CR network, the Secondary (or unlicensed) User (SU) is allowed to opportunistically access the spectrum "holes" that are not occupied by the Primary (or licensed) User (PU). Generally, the SUs constantly observe the spectrum bands by performing spectrum sensing. Once a spectrum "hole" is discovered, an SU could temporarily transmit on this part of the spectrum. Upon the presence of a PU in this part of the spectrum, however, the SU has to switch to another available spectrum band by performing spectrum handoff, avoiding interference with the PU transmission. The development of CR technology leads to the new communications paradigm called Dynamic Spectrum Access (DSA), which relaxes the traditional fixed spectrum assignment policy and al- lows a CR networks to temporally "borrow" a part of the spectrum from the primary network. As a consequence, the scarce spectrum resources are shared, in a highly efficient and resilient fashion, between the primary network and the CR network.802.22 is also called wireless radio area network (WRAN) or cognitive radio network (CRN) by IEEE. Cognitive Radio (CR) is further enhance as compared to SDR by employing software for measurement of the vacant portion of the wireless spectrum which is already there and operate that spectrum in a way that bound the interfering with other devices. Licensed user is stated to be as a primary or key user in dynamic spectrum Access (DSA). The user who didn't have any licensed that got the permission for spectrum opportunistically is referred to as secondary user [4]. Cognitive Radio (CR) is more flexible and exposed to wireless network, if we compared with the typical radio networks. When the result of spectrum sensing in altered maliciously network activities which are normal will be disabled, even whole traffic may be broken down. CR is the main technique which realizes DSA policy. CR first senses and identify the spectrum which is scanning a certain range of the spectrum to unoccupied spectrum. This methodology is used for the secondary user can

determine that which spectrum can be used either radio or not.

There are four fundamental functions which the CRN device must perform, as stated below:-

- Spectrum sensing identifies the parts of the accessible spectrum and senses the presence of the PU operating in the licensed band.
- Spectrum management determines the best channel to establish communication.
- Spectrum sharing sets up a coordination access among users on the selected channel.
- Spectrum mobility vacates the channel in case the PU is detected

Research focus

Our research work focuses on detecting and preventing the below mentioned attacks of Cognitive Radio Network:

1) Firstly, detects the SSDF(spectrum sensing data falsification) attack of link layer and prevents the attacker sending false local spectrum sensing results to its neighbours or to the fusion centre.,

2) Secondly, detects the Control Channel Saturation DoS attack of link layer, and helps to avoid forged MAC control frames for the purpose of saturating the control channel that decreases the network performance due to Link layer collisions.,

3) Thirdly, detects the SCN(selfish channel negotiation) attack of ink layer, and prevents the selfish host in order to maintain the end-to-end throughput of the whole CRN.,

4) Finally, detects the Worm Hole, Sink Hole and Hello Flood Attacks of network layer to prevent the routing loops of the network by saving power and energy.

MOTIVATION

Cognitive Radio (CR) is a promising technology for next-generation wireless networks in order to efficiently utilize the limited spectrum resources and satisfy the rapidly increasing demand for wireless applications and services. It solves the spectrum scarcity problem by allocating the spectrum dynamically to unlicensed users. It uses the free spectrum bands which are not being used by the licensed users without causing interference to the incumbent transmission. So, spectrum sensing is the essential mechanism on which the entire communication depends. Cognitive radio networks introduce new classes of security threats and challenges, such as licensed user emulation attacks in spectrum sensing and misbehaviors in the common control channel transactions, which degrade the overall network operation and performance. So that it causes the crucial threat in the cognitive radio network.

PROPOSED METHODOLOGY

The objective of the research work is to propose several efficient methods like ***Machine learn- ing based defense technique, cross layer optimization and defence based prevention mechanisms*** to overcome the drawbacks of the existing mechanisms to detect and prevent the attacks such as **SSDF**(spectrum sensing data falsification),**Control Channel Saturation DoS** (denial of service), **SCN**(selfish channel negotiation), **Worm Hole, Sink Hole and Hello Flood Attacks** in link layer and network layer of ***Cognitive Radio Networks***.

The proposed methodology consists of following steps:

Machine Learning based Defense: One critical part of defense against the several attacks in data link layer and network layer is to analyze data and dig out useful information related with users' behaviors, while machine learning provides powerful data mining tools to achieve this task. In fact, there are already several preliminary studies using various machine learning methods, such as *clustering algorithms* (see, e.g., [37]) and *pattern extraction algorithms* (see, e.g., [37]), to defense against the attacks. Using machine learning algorithms various attacks in network is detected and prevented.

Prevention based Defense: Traditional detection based defense is reactive and may not satisfy various needs of security, while prevention based defense provides the problems with a more flexible and proactive solution. Specifically, prevention based defence, a promising kind of defense schemes, is regarded as one aiming to increase difficulty and risks of attack behaviors and actively develop the defender's advantages, which may contain such two factors:

- ***Prevention before attack.*** it selectively improve critical nodes' security levels. In consequence, the attack cost is increased while attack effectiveness declines.

- ***Appropriate counterattack***. First of all, offending is coordinated with traditional defense schemes including bad data detection. After a certain period, the knowledge of malicious users' behaviors are gradually obtained and the network develops the capacity of launching counterattack. Here, the counterattack means that users identified as malicious ought to be in certain punishment, which will improve users' responsibility widely neglected by users due to the openness of the underlying protocols.

Optimization of the proposed methodology:

1) ***Universal Defense:*** Generally, majority of existing defense algorithms have been designed for specific attack models and perform well only under specific attack parameters. To our best knowledge, a generalised approach for data link layer and network layer attack modeling, the *data cleansing-based defence* scheme developed has been shown to perform well under various attack parameters via computer simulations. One key challenge is that: due to the *spear-and- shield relation* between the attacks and defense, the defence system cannot obtain cooperation from the hostile attackers, and thus do not know the specific attack model and parameters before deploying the proper defense algorithm. Consequently, ***attack pattern/model recognition*** and ***attack parameter estimation*** are suggested as two key techniques for the design of a practical and universal defense scheme.

2) ***Optimal Attack:*** The optimal attack is considered to have the ability to optimize attack performances of attacker(s), at the same time, generally serves as the worst case for the design of a robust defense system. For every rational attacker, the possible goals to launch an attack mainly include: i) maximization of the attack gain (i.e., the destructive to CSS), ii) minimization of the attack cost (e.g., time and energy consumption), and iii) minimization of the attack risk (e.g., being captured and punished).

CONCLUSION

Although a number of studies have been done on several types of data link and network layer attacks and defenses for CSS in CRNs, there are still a number of challenges unsolved and open issues waiting for solutions. Specifically, from the perspective of attackers, when launching the attack, users have to take into account of the factors of attack gain, attack cost and attack risk, together. from the perspective of defenders, there are also three aspects deserving consideration: defense reliability, defense efficiency and defense universality. The attacks and defenses are mutually coupled from each other. Attackers need to adjust their strategies to keep their negative effects on final decisions and avoid defenders' detection, while defenders have to learn and analyze attack behaviors and designs effective defense rules. Indeed, attack and defense ought to be considered together. the proposed methodology overcomes the problems of several data link and network layer attacks and it effects in CSS(Co-operative Spectrum Sensing) of CNRs using Ma- chine Learning based Defense, Cross layers optimization techniques and Defence based Prevention mechanisms.

ACKNOWLEDGEMENT

The author thanks Prof. S.Sridhar, Ex. Vice Chancellor, Dr. K.N.Modi University, Rajasthan, for communicating this article to this Journal for publication.

REFERENCES

[1]. 'The Design of a Defense Mechanism to Mitigate the Spectrum Sensing Data Falsification attack in Cognitive Radio Ad Hoc Networks',2016 IEEE.

[2]. A.Hyils Sharon Magdalene, Dr. L. Thulasimani,Fuzzy Clustering Means (FCM) for mitigating Spectrum sensing data falsification (SSDF) attack in Cognitive Radio Networks ', 2017 IEEE International Conference on Computational Intelligence and Computing Research.

[3]. Abbas Ali Sharifi and Mir Javad Musevi Niya, Member, IEEE, 'Defense Against SSDF Attack in Cognitive Radio Networks: Attack-Aware Collaborative Spectrum Sensing Approach', IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 1, JANUARY 2016 .

[4]. Alireza Attar, Helen Tang, Senior Member IEEE, Athanasios V. Vasilakos, Senior Member IEEE, F. Richard Yu, Senior Member IEEE, and Victor C. M. Leung,Fellow IEEE, 'A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions', Proceedings of the IEEE | Vol. 100, No. 12, December 2012 0018-9219.

[5]. Anil Kumar and Dr. Rajendra Kumar, 'Simulation Analysis of GLRT and Eigenvalue Based Methods for Cognitive Radio', 2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India.

[6]. EI Qingqi, LI Hongning and LIU Xianjun , 'Neighbor Detection-Based Spectrum Sensing Algorithm in Distributed Cognitive Radio Networks', Chinese Journal of Electronics Vol.26, No.2, Mar. 2017.

[7]. Fang Ye and Xun Zhang, 'Evidence-theory-based Collaborative Spectrum Sensing with Efficient reditability Evaluation in Cognitive Radio Networks', 2017 Progress In Electromagnetics Research Symposium — Fall (PIERS — FALL), Singapore, 19–22 November.

[8]. GUANGMING NIE, GUORU DING (Senior Member, IEEE), LINYUAN ZHANG, AND QIHUI WU , (Senior

Member, IEEE) , 'Byzantine Defense in Collaborative Spectrum Sensing via Bayesian Learning'.

[9]. Headar Tarsh Batool, Dr. R.S.Kawitkar, 'Performance Investigation of Insistent Spectrum Sensing Data Falsification on Cognitive Radio Networks',Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS 2018).

[10]. Huifang Chen, Member, IEEE, Ming Zhou, Lei Xie, Member, IEEE, and Jie Li, Senior Member, IEEE, 'Cooperative Spectrum Sensing With M-Ary Quantized Data in Cognitive Radio Networks Under SSDF Attacks',IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 16, NO. 8, AUGUST 2017.

[11]. Huifang Chen, Member, IEEE, Ming Zhou, Lei Xie, Member, IEEE, Kuang Wang, and Jie Li, Senior Member, IEEE, 'Joint Spectrum Sensing and Resource Allocation Scheme in Cognitive Radio Networks with Spectrum Sensing Data Falsification Attack',IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 65, NO. 11, NOVEMBER 2016.

[12]. Ismail K. Ahmed and Abraham O. Fapojuwo, 'Security Threat Assessment of Simultaneous Multiple Denial–of–Service Attacks in IEEE 802.22 Cognitive Radio Networks', 2016 IEEE.

[13]. Issah Ngomane, Mthulisi Velempini, Sabelo Velemseni Dlamini, ' Trust-based System to Defend Against the Spectrum Sensing Data Falsification Attack in Cognitive Radio Ad Hoc Network', 2018 IEEE.

[14]. Izhar Ahmed Sohu , Asif Ahmed Rahimoon, Amjad Ali junejo, Sadam Hussain junejo,Arsalan Ahmed Sohu 'Analogous Study of Security Threats in Cognitive Radio', International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2019.

[15]. Ji Wang,Ing-Ray Chen, Jeffrey J.P, Ding-Chau Wang, 'SSDF Attacks in Distributed Cognitive Radio Networks' .

[16]. Jianwu, FENG Zhiyong, ZHANG Ping,'A Survey of Security Issues in Cognitive Radio Networks', Beijing University of Posts and Telecommunications, Beijing 100876, China.

[17]. JIANXIN DAI , JUAN LIU, CUNHUA PAN , JIANGZHOU WANG, (Fellow, IEEE), CHONGHU CHENG, and ZHILIANG HUANG, ' MAC Based Energy Efficiency in Cooperative Cognitive Radio Network in the Presence of Malicious Users', 2169-3536- 2018 IEEE,Digital Object Identifier 10.1109/ACCESS.2018.2793906.

[18]. John Kelly, Jonathan Ashdown , 'Spectrum Sensing Falsification Detection in Dense Cognitive Radio Networks using a Greedy Method', Air Force Research Laboratory (AFRL) Information Directorate Rome, 2019.

[19]. Jun Wu, Tiecheng Song, Cong Wang, Yue Yu, Miao Liu, Jing Hu , 'Robust Cooperative Spectrum Sensing Against Probabilistic SSDF Attack in Cognitive Radio Networks', National Mobile Communication Research Lab Southeast University, Nanjing, China.

[20]. Jun Wu, Xi Li, Tiecheng Song, Lei Zhang, Miao Liu, Jing Hu, 'Two-stage Credit Threshold on Cooperative Spectrum Sensing to Exclude Malicious Users in Mobile Cognitive Radio Networks', National Mobile Communication Research Lab Southeast University, Nanjing, China.

[21]. Lanka Sejaphala, Mthulisi Velempini, Sabelo Velemseni Dlamini 'HCOBASAA: Countermeasure Against Sinkhole Attacks in Software-Defined Wireless Sensor Cognitive Radio Network', 2018 IEEE.

[22]. Linyuan Zhang, Guoru Ding, Member, IEEE, Qihui Wu, Senior Member, IEEE, Yulong Zou, Senior Member, IEEE, Zhu Han, Fellow, IEEE, and Jinlong Wang, Senior Member, IEEE, 'Byzantine Attack and Defense in Cognitive Radio Networks: A Survey'.

[23]. Moinul Hossain and Jiang Xie, 'Off-sensing and Route Manipulation Attack: A Cross-Layer Attack in Cognitive Radio based Wireless Mesh Networks', IEEE INFOCOM 2018 - IEEE Conference on Computer Communications.

[24]. Natasha Saini, Nitin Pandey, Ajeet Pal Singh, 'Analyzing and Developing Security Techniques for Worms in Cognitive Networks', 2016 IEEE International Conference on Computational Intelligence and Computing Research.

[25]. Natasha, Nitin Pandey, Ajeet Pal Singh, 'Formal Approach to Security Techniques in Cognitive Networks', 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).

[26]. Networks Roshni Rajkumari and Ningrinla Marchang, Member, IEEE, 'Secure Non-Consensus Based Spectrum Sensing in Non-Centralized Cognitive Radio', IEEE SENSORS JOURNAL, VOL. 18, NO. 9, MAY 1, 2018.

[27]. Ohrid, Macedonia Pujue Wang, Cailian Chen, Shanying Zhu, Ling Lyu, Weidong Zhang, and Xinping Guan, 'An Optimal Reputation-based Detection against SSDF Attacks in Industrial Cognitive Radio Network', 2017 13th IEEE International Conference on Control & Automation (ICCA) July 3-6, 2017.

[28]. Pinaki Sankar Chatterjee,Monideepa Roy, 'Lightweight cloned-node detection algorithm for efficiently handling SSDF attacks and facilitating secure spectrum allocation in CWSNs',IET Wirel. Sens. Syst., 2018, Vol. 8 Iss. 3, pp. 121-128 © The Institution of Engineering and Technology 2018.

[29]. Ping Bai, Xun Zhang, and Fang Ye, 'Reputation-based Beta Reputation System against SSDF Attack in Cognitive Radio Networks', 2017 Progress In Electromagnetics Research Symposium — Fall (PIERS — FALL), Singapore, 19–22 November.

[30]. Rajesh K. Sharma, Member, IEEE, and Danda B. Rawat, Senior Member, IEEE, 'Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey', IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 2, SECOND QUARTER 2015.

[31]. Ramesh babu B, Meenakshi Tripathi , Manoj Singh Gaur, Dinesh Gopalani, Dharm Singh Jat, 'Cognitive Radio Ad-Hoc Networks: Attacks and Its Impact'.

[32]. Ruiyan Du , Ying Zhou, Fulai Liu, Xinwei Wang' 'An Effective Collaborative Spectrum Sensing Method against SSDF Attack', 2017 IEEE.

[33]. Sasa Maric, Leonardo Goratti ' A Simple and Highly Effective SSDF attacks Mitigation Method', 2016 IEEE.

[34]. Shikhamoni Nath, Ningrinla Marchang and Amar Taggu, 'Mitigating SSDF Attack using K-Medoids Clustering in Cognitive Radio Networks', 2015 Eight International Workshop on Selected Topics in Mobile and Wireless Computing.

[35]. Shuai Yuan, Lei Li and Chunxiao Chigan, 'On MMD-based Secure Fusion Strategy for Robust Cooperative Spectrum Sensing', DOI 10.1109/TCCN.2019.2906236, IEEE Transactions on Cognitive Communications and Networking.

[36]. Suchismita Bhattacharjee, Raiping Keitangnao, Ningrinla Marchang, 'Association Rule Mining for Detection of Colluding SSDF Attack in Cognitive Radio Networks', 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016, Coimbatore, INDIA.

[37]. Sukanya Chatterjee, Pinaki S Chatterjee A Comparison based Clustering Algorithm to Counter SSDF attack in CWSN. 2015 International Conference on Computational Intelligence & Networks.

[38]. Ting Peng, Yuebin Chen, Jie Xiao,Yang Zheng, Jiangfeng Yang, ' Improved Soft Fusion-Based Cooperative Spectrum Sensing Defense Against SSDF Attacks', 2016 IEEE.

[39]. Xuekang Sun, Rikang Zhou, Hongxing Wu, Li Gao,Yuyan Zhang, 'Angle based Malicious User Detection for Wideband Cognitive Radio Network', The 20th International Symposium on Wireless Personal Multimedia Communications (WPMC-2017).

[40]. Yasir Al-Mathehaji, Said Boussakta, Martin Johnston, and Harith Fakhrey,'Defeating SSDF Attacks With Trusted Nodes Assistance in Cognitive Radio Networks' July 19, 2017.

[41]. Yu Gan, Chunxiao Jiang, Senior Member, IEEE, Norman C. Beaulieu, Fellow, IEEE, Jian Wang, Member, IEEE, and Yong Ren, Senior Member, IEEE, 'Secure Collaborative Spectrum Sensing: A Peer-Prediction Method',IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 64, NO. 10, OCTOBER 2016.

[42]. Zhixu Cheng, Tiecheng Song, Jing Zhang, Jing Hu, Yazhou Hu, Lianfeng Shen, Xi Li, Jun Wu, 'Self-Organizing Map-Based Scheme Against Probabilistic SSDF Attack in Cognitive Radio Networks', National Mobile Communications Research Laboratory, Southeast University Nanjing, Jiangsu, 210096, China.

